(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2021 (18.03.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/049874 A1

(51) International Patent Classification:
H04W 12/06 (2009.01) *H04W 4/40* (2018.01)
H04W 8/24 (2009.01) *H04W 84/06* (2009.01)
H04W 60/00 (2009.01)

(21) International Application Number:
PCT/KR2020/012175

(22) International Filing Date:
09 September 2020 (09.09.2020)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2019-0111755 09 September 2019 (09.09.2019) KR

(71) Applicant: **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

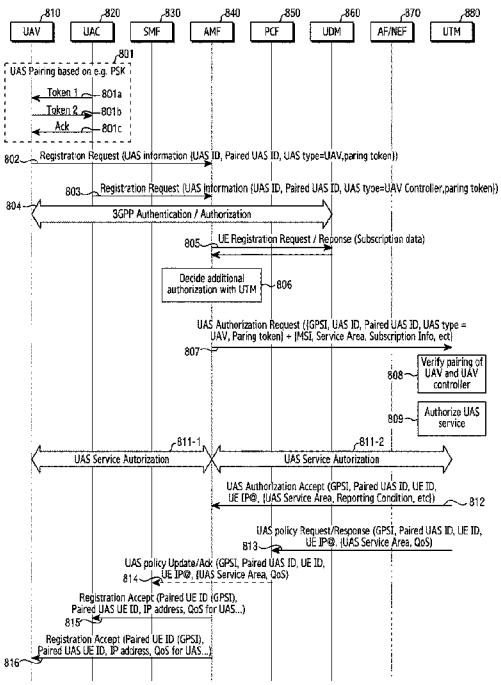
(72) Inventors: **PARK, Jungshin**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR). **HAN, Yoonseon**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR). **MOON, Sangjun**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR). **JEONG, Sangsoo**; 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do 16677 (KR).

(74) Agent: **KWON, Hyuk-Rok** et al.; 2F, 28, Gyeonghuigung-gil, Jongro-gu, Seoul 03175 (KR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: APPARATUS AND METHOD FOR AUTHENTICATION AND AUTHORIZATION FOR UNMANNED AERIAL SERVICE IN WIRELESS COMMUNICATION SYSTEM



(57) Abstract: The present disclosure relates to a pre-5th-Generation (5G) or 5G communication system to be provided for supporting higher data rates Beyond 4th-Generation (4G) communication system such as Long Term Evolution (LTE). The disclosure relates to a method and an apparatus for authenticating an unmanned aerial service (UAS) terminal using a mobile communication system and authorizing a UAS in consideration of information about pairing between UAS terminals. According to a provided method, a UAS operator can authenticate a UAS terminal using a mobile communication system without any additional process and can control a UAS to be provided between an unmanned aerial vehicle (UAV) and a UAV controller (UAC) which are allowed by the operator.

WO 2021/049874 A1

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

Description

Title of Invention: APPARATUS AND METHOD FOR AUTHENTICATION AND AUTHORIZATION FOR UNMANNED AERIAL SERVICE IN WIRELESS COMMUNICATION SYSTEM

Technical Field

[1] The disclosure generally relates to a wireless communication system. More particularly, the disclosure relate to an apparatus and a method for authentication and authorization for an unmanned aerial service (UAS) using a wireless communication system.

Background Art

[2] To meet the demand for wireless data traffic having increased since deployment of 4th generation (4G) communication systems, efforts have been made to develop an improved 5th generation (5G) or pre-5G communication system. Therefore, the 5G or pre-5G communication system is also called a 'Beyond 4G Network' or a 'Post Long Term Evolution (LTE) System'.

[3] The 5G communication system is considered to be implemented in higher frequency (mmWave) bands, e.g., 60GHz bands, so as to accomplish higher data rates. To decrease propagation loss of the radio waves and increase the transmission distance, the beamforming, massive multiple-input multiple-output (MIMO), Full Dimensional MIMO (FD-MIMO), array antenna, an analog beam forming, large scale antenna techniques are discussed in 5G communication systems.

[4] In addition, in 5G communication systems, development for system network improvement is under way based on advanced small cells, cloud Radio Access Networks (RANs), ultra-dense networks, device-to-device (D2D) communication, wireless backhaul, moving network, cooperative communication, Coordinated Multi-Points (CoMP), reception-end interference cancellation and the like.

[5] In the 5G system, Hybrid frequency shift keying (FSK) and quadrature amplitude modulation (FQAM) and sliding window superposition coding (SWSC) as an advanced coding modulation (ACM), and filter bank multi carrier (FBMC), non-orthogonal multiple access (NOMA), and sparse code multiple access (SCMA) as an advanced access technology have been developed.

[6] With the development of wireless communication systems, such as a 5G system, it is expected to be able to provide various services. Therefore, there is a need for methods for smoothly providing these services.

[7] The above information is presented as background information only to assist with an understanding of the disclosure. No determination has been made, and no assertion is

made, as to whether any of the above might be applicable as prior art with regard to the disclosure.

Disclosure of Invention

Technical Problem

[8] The embodiments herein is to provide a method and an apparatus for authenticating a terminal and for authorizing a service in order to provide an unmanned aerial service (UAS) in a wireless communication system.

Solution to Problem

[9] According to various embodiments, an operating method of an apparatus for an access management function (AMF) in a wireless communication system may include: receiving a registration request message associated with an unmanned aerial service (UAS) of a terminal from the terminal; performing an authentication process of the terminal; requesting registration of the terminal from a user data management (UDM); receiving a response to a request for the registration of the terminal from the UDM; determining whether to perform additional authentication; requesting UAS authentication of the terminal from a UAS traffic management (UTM); receiving a result of the UAS authentication of the terminal from the UTM; and transmitting a registration acceptance message to the terminal.

[10] According to various embodiments, an operating method of an apparatus for a UTM in a wireless communication system may include: receiving a request for authentication associated with a UAS from an AMF; identifying a pair of paired terminals; identifying whether pairing tokens match; performing a UAS authentication process; and transmitting a result of UAS authentication of a terminal to the AMF.

[11] According to various embodiments, an operating method of a terminal in a wireless communication system may include: performing mutual authentication with a different terminal by a predetermined pairing method; requesting registration associated with a UAS from an AMF; and receiving a result of requesting the registration from the AMF.

[12] According to various embodiments, an apparatus for an AMF in a wireless communication system may include: a transceiver; and at least one processor, wherein the at least one processor may be configured to: receive a registration request message associated with a UAS of a terminal from the terminal; perform an authentication process of the terminal; request registration of the terminal from a UDM; receive a response to a request for the registration of the terminal from the UDM; determine whether to perform additional authentication; request UAS authentication of the terminal from a UTM; receive a result of the UAS authentication of the terminal from the UTM; and transmit a registration acceptance message to the terminal.

[13] According to various embodiments, an apparatus for a UTM in a wireless communication system may include: a transceiver; and at least one processor, wherein the at least one processor may be configured to: receive a request for authentication associated with a UAS from an AMF; identify a pair of paired terminals; identify whether pairing tokens match; perform a UAS authentication process; and transmit a result of UAS authentication of a terminal to the AMF.

[14] According to various embodiments, a terminal in a wireless communication system may include: a transceiver; and at least one processor, wherein the at least one processor may be configured to: perform mutual authentication by generating a pairing token and exchanging the pairing token with a different terminal; request registration associated with a UAS from an AMF; and receive a result of requesting the registration from the AMF.

[15] An apparatus and a method according to various embodiments enable an unmanned aerial service (UAS) operator to use a mobile communication system when authorizing a UAS for a UAS terminal, thereby controlling the UAS to be provided between UAS terminals allowed for pairing.

Brief Description of Drawings

[16] The above and other aspects, features, and advantages of certain embodiments of the disclosure will be more apparent from the following description taken in conjunction with the accompanying drawings, in which:

[17] FIG. 1 illustrates an unmanned aerial service (UAS) system according to various embodiments;

[18] FIG. 2 illustrates the configuration of an aerial terminal according to various embodiments;

[19] FIG. 3 illustrates the configuration of a controlling terminal in a wireless communication system according to various embodiments;

[20] FIG. 4 illustrates the configuration of a core network device in a wireless communication system according to various embodiments;

[21] FIG. 5 is a flowchart illustrating the operation of an access management function (AMF) in a wireless communication system according to various embodiments;

[22] FIG. 6 is a flowchart illustrating the operation of a UAS traffic management (UTM) in a wireless communication system according to various embodiments;

[23] FIG. 7 is a flowchart illustrating the operation of a UAS terminal in a wireless communication system according to various embodiments;

[24] FIG. 8 is a signal exchange diagram showing that a UAS terminal performs authentication for a UAS in a wireless communication system according to various embodiments;

[25] FIG. 9 is a signal exchange diagram showing that a UAS terminal performs initial access in a wireless communication system according to various embodiments; and

[26] FIG. 10 is a signal exchange diagram showing that a UAS terminal having completed access performs authentication for a UAS in order to use the UAS in a wireless communication system according to various embodiments.

Best Mode for Carrying out the Invention

[27] It may be advantageous to set forth definitions of certain words and phrases used throughout this patent document: the terms "include" and "comprise," as well as derivatives thereof, mean inclusion without limitation; the term "or," is inclusive, meaning and/or; the phrases "associated with" and "associated therewith," as well as derivatives thereof, may mean to include, be included within, interconnect with, contain, be contained within, connect to or with, couple to or with, be communicable with, cooperate with, interleave, juxtapose, be proximate to, be bound to or with, have, have a property of, or the like; and the term "controller" means any device, system or part thereof that controls at least one operation, such a device may be implemented in hardware, firmware or software, or some combination of at least two of the same. It should be noted that the functionality associated with any particular controller may be centralized or distributed, whether locally or remotely.

[28] Moreover, various functions described below can be implemented or supported by one or more computer programs, each of which is formed from computer readable program code and embodied in a computer readable medium. The terms "application" and "program" refer to one or more computer programs, software components, sets of instructions, procedures, functions, objects, classes, instances, related data, or a portion thereof adapted for implementation in a suitable computer readable program code. The phrase "computer readable program code" includes any type of computer code, including source code, object code, and executable code. The phrase "computer readable medium" includes any type of medium capable of being accessed by a computer, such as read only memory (ROM), random access memory (RAM), a hard disk drive, a compact disc (CD), a digital video disc (DVD), or any other type of memory. A "non-transitory" computer readable medium excludes wired, wireless, optical, or other communication links that transport transitory electrical or other signals. A non-transitory computer readable medium includes media where data can be permanently stored and media where data can be stored and later overwritten, such as a rewritable optical disc or an erasable memory device.

[29] Definitions for certain words and phrases are provided throughout this patent document, those of ordinary skill in the art should understand that in many, if not most instances, such definitions apply to prior, as well as future uses of such defined words

and phrases.

[30] FIGS. 1 through 10, discussed below, and the various embodiments used to describe the principles of the present disclosure in this patent document are by way of illustration only and should not be construed in any way to limit the scope of the disclosure. Those skilled in the art will understand that the principles of the present disclosure may be implemented in any suitably arranged system or device.

[31] The terms used herein are merely for the purpose of describing particular embodiments and are not intended to limit the scope of other embodiments. As used herein, singular forms may include plural forms as well unless the context clearly indicates otherwise. Unless defined otherwise, all terms used herein, including technical and scientific terms, have the same meanings as those commonly understood by a person skilled in the art to which the disclosure pertains. Such terms as those defined in a generally used dictionary may be interpreted to have the meanings equal to the contextual meanings in the relevant field of art, and are not to be interpreted to have ideal or excessively formal meanings unless clearly defined in the disclosure. In some cases, even the terms defined in the disclosure should not be interpreted to exclude embodiments of the disclosure.

[32] In various embodiments of the disclosure to be described below, hardware approaches will be illustrated by way of example. However, various embodiments of the disclosure encompass techniques using both hardware and software and thus are not to be construed as excluding a software-based approach.

[33] The disclosure relates to a method and an apparatus for authentication for an unmanned aerial service (UAS) in a wireless communication system. Specifically, the disclosure illustrates a technique for authenticating a terminal and for authorizing a service in order to provide a UAS in a wireless communication system.

[34] As used herein, terms for identifying access nodes, terms referring to network entities, terms referring to messages, terms referring to interfaces between network entities, terms referring to various types of identification information, and the like are used for convenience of explanation. Therefore, the disclosure is not limited by the following terms, and other terms having equivalent technical meanings may be used.

[35] In the following description, a physical channel and signal may be interchangeable with a data or control signal. For example, although a physical downlink shared channel (PDSCH) is a term referring to a physical channel in which data is transmitted, a PDSCH may also be used to refer to data. That is, in the disclosure, the expression "a physical channel is transmitted" may be interpreted equally as the expression "data or a signal is transmitted through a physical channel".

[36] In the disclosure, higher-layer signaling refers to a method of signal transmission from a base station to a terminal using a downlink data channel of a physical layer or

from a terminal to a base station using an uplink data channel of a physical layer. Higher-layer signaling may be understood as radio resource control (RRC) signaling or a media access control (MAC) control element (CE).

[37] Further, although the disclosure illustrates various embodiments using terms used in some communication standards (e.g., 3rd Generation Partnership Project (3GPP)), these standards are provided merely for convenience of description. Various embodiments of the disclosure may be easily modified and applied to other communication systems.

[38] FIG. 1 illustrates a UAS system 100 according to various embodiments.

[39] Referring to FIG. 1, the UAS system 100 includes a controlling terminal 113, an aerial terminal 115, a radio access network (RAN) 130, a core network (CN) 150, a UAS traffic management (UTM) 170, and a regulator 190.

[40] The controlling terminal 113 and the aerial terminal 115 are terminals for a UAS 110. The controlling terminal 113 may access a CN 150a through an RAN 130a, and the aerial terminal 115 may access a CN 150b through an RAN 130b. The aerial terminal 115 is a device capable of unmanned flight by remote control. The controlling terminal 113 is a device to control the aerial terminal 115, and may transmit an instruction to control the aerial terminal 115 according to a user's manipulation. The aerial terminal 115 may be referred to as an unmanned aerial vehicle (UAV), a drone, an aerial user equipment (UE), or other terms with equivalent technical meanings. The controlling terminal 113 may be referred to as a UAV controller (UAC), a remote control device, a controlling UE, or other terms with equivalent technical meanings. In addition, the controlling terminal 113 and the aerial terminal 115 may be collectively referred to as a UAS terminal.

[41] The RAN 130 is a network that is directly connected to a user device (e.g., the controlling terminal 113, the aerial terminal 115, and the like) and is infrastructure providing wireless access for the controlling terminal 113 and the aerial terminal 115. The RAN 130 includes a set of a plurality of base stations, and the plurality of base stations may perform communication through interfaces established therebetween. At least some of the interfaces between the plurality of base stations may be wired or wireless. The base stations may have a structure in which a central unit (CU) and a distributed unit (DU) are separated. In this case, one CU may control a plurality of DUs. Here, the base stations may be referred to as an access point (AP), an eNodeB (eNB), a 5th-generation (5G) node, a next-generation nodeB (gNB), a wireless point, a transmission/reception point (TRP), or other terms with equivalent technical meanings, in addition to a base station.

[42] The CN 150 is a network that manages a system, controls the RAN 130, and processes data and control signals for the terminals 113 and 115 transmitted and

received through the RAN 130. The CN 150 performs various functions, such as control of a user plane and a control plane, mobility processing, subscriber information management, billing, and interworking with other types of systems (e.g., a long-term evolution (LTE) system). To perform these various functions, the CN 150 may include a plurality of functionally separated entities having different network functions (NFs). For example, the CN 150 may include at least one of a session management function (SMF), an access management function (AMF), a policy control function (PCF), and a user data management (UDM). The listed functional entities may be configured as at least one hardware device (e.g., a server). When functions of a plurality of functional entities are performed in one device, the plurality of functional entities may be configured as a plurality of virtual machines.

[43] The UTM 170 provides additional information for the UAS 110 and performs a function for controlling an operation. The UTM 170 periodically collects information about a location change of a UAS terminal from the UAS terminal and a mobile communication network in order to track and manage registration and movement of the UAS terminal, that is, each of the aerial terminal 115 and the controlling terminal 113, and performs an operation necessary to control the aerial terminal 115, such as stopping flight of the terminal or controlling the terminal to fly back to a flight-allowed zone when the terminal deviates from the flight-allowed zone, considering flight control information designated by the regulator 190. Further, the UTM 170 receives information for authentication of the UAS terminal and service authorization from the UAS terminal and the mobile communication system and determines whether to authorize a UAS.

[44] The regulator 190 provides the flight control information to the UTM 170. The regulator 190 may be a server including a storage device that stores flight control information. The flight control information is defined by a network operator or a third party (e.g., a government) and may be input to the regulator 190.

[45] FIG. 2 illustrates the configuration of an aerial terminal according to various embodiments. The configuration illustrated in FIG. 2 may be understood as the configuration of the aerial terminal 115. The terms 'unit', '-or/er', and the like used herein indicate a unit for processing at least one function or operation, which may be implemented as hardware, software, or a combination thereof.

[46] Referring to FIG. 2, the aerial terminal includes a driver 210, a sensor unit 220, a communication unit 230, a storage unit 240, and a controller 250.

[47] The driver 210 generates physical power to fly the aerial terminal in the air and to move the aerial terminal in the air. To this end, the driver 210 may include at least one motor, at least one propeller, and the like.

[48] The sensor unit 220 collects sensing data necessary for position control and driving

of the aerial terminal. The sensor unit 220 may collect data in order to determine the direction, slope, altitude, and location of the aerial terminal and the distance of the aerial terminal from a different object (e.g., a wall or the ground). To this end, the sensor unit 220 may include at least one of a magnetic force sensor, an acceleration sensor, a gyroscope, a barometric pressure sensor, a global positioning system (GPS) sensor, a distance sensor, an inertial measurement unit (IMU), and a vision sensor.

[49] The communication unit 230 performs functions for transmitting or receiving a signal through a wireless channel. For example, the communication unit 230 performs a function of conversion between a baseband signal and a bit stream according to the physical-layer specification of a system. For example, in data transmission, the communication unit 230 encodes and modulates a transmitted bit stream to generate complex symbols. Further, in data reception, the communication unit 230 demodulates and decodes a baseband signal to reconstruct a received bit stream. The communication unit 230 upconverts a baseband signal into a radio-frequency (RF) band signal, and may transmit the RF band signal through an antenna. The communication unit 230 downconverts an RF band signal, received through the antenna, into a baseband signal. In one example, the communication unit 230 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a DAC, an ADC, or the like.

[50] The communication unit 230 may include a plurality of transmission/reception paths. In addition, the communication unit 230 may include at least one antenna array including a plurality of antenna elements. From the aspect of hardware, the communication unit 230 may include a digital circuit and an analog circuit (e.g., a radio-frequency integrated circuit (RFIC)). Here, the digital circuit and the analog circuit may be configured as a single package. Further, the communication unit 230 may include a plurality of RF chains. The communication unit 230 may perform beamforming.

[51] The communication unit 230 may include different communication modules to process signals in different frequency bands. Furthermore, the communication unit 230 may include a plurality of communication modules to support a plurality of different radio access technologies. For example, the different radio access technologies may include Bluetooth Low Energy (BLE), Wireless Fidelity (Wi-Fi), Wi-Fi Gigabyte (WiGig), a cellular network (e.g. long-term evolution (LTE)), and the like. The different frequency bands may include a super-high-frequency (SHF) band (e.g., 2.5 GHz or 5 GHz) and a millimeter (mm)-wave band (e.g., 60 GHz).

[52] As described above, the communication unit 230 transmits and receives a signal. Accordingly, part or all of the communication unit 230 may be referred to as a transmitter, a receiver, or a transceiver. In the following description, transmission and

reception performed through a wireless channel are construed as including processing performed as described above by the communication unit 230.

[53] The storage unit 240 stores data, such as a default program, an application, and setting information, for the operation of the aerial terminal. The storage unit 240 may be configured as volatile memory, nonvolatile memory, or a combination of volatile memory and nonvolatile memory. The storage unit 240 provides the stored data in response to a request from the controller 250.

[54] The controller 250 controls the overall operation of the aerial terminal. For example, the controller 250 controls the driver 210, thereby controlling the flight of the aerial terminal. Here, the controller 250 may use the sensing data provided from the sensor unit 220. Further, the controller 250 transmits and receives a signal through the communication unit 230. Here, the controller 250 may receive a control command message transmitted from a controlling terminal (e.g., the controlling terminal 113) through the communication unit 230. In addition, the controller 250 records and reads data in the storage unit 240. The controller 250 may perform functions of a protocol stack required by communication standards. To this end, the controller 250 may include at least one process or microprocessor, or may be part of a processor. Part of the communication unit 230 and the controller 250 may be referred to as a communication processor (CP). According to various embodiments, the controller 250 may control the aerial terminal to perform operations according to various embodiments described below.

[55] Although not shown in FIG. 2, the aerial terminal may further include a camera, a display, and the like in addition to the aforementioned components. When a camera is included, the controller 250 may transmit an image captured by the camera to the controlling terminal through the communication unit 230. When a display is included, the controller 250 may display information about the status of the aerial terminal on the display or may display a screen for configuring the aerial terminal.

[56] FIG. 3 illustrates the configuration of a controlling terminal in a wireless communication system according to various embodiments. The configuration illustrated in FIG. 3 may be understood as the configuration of the controlling terminal 113. The terms 'unit', '-or/er', and the like used herein indicate a unit for processing at least one function or operation, which may be implemented as hardware, software, or a combination thereof.

[57] Referring to FIG. 3, the controlling terminal includes a communication unit 310, a user interface unit 320, a storage unit 330, and a controller 340.

[58] The communication unit 310 performs functions for transmitting or receiving a signal through a wireless channel. For example, the communication unit 310 performs a function of conversion between a baseband signal and a bit stream according to the

physical-layer specification of a system. For example, in data transmission, the communication unit 310 encodes and modulates a transmitted bit stream to generate complex symbols. Further, in data reception, the communication unit 310 demodulates and decodes a baseband signal to reconstruct a received bit stream. The communication unit 310 upconverts a baseband signal into a radio-frequency (RF) band signal, and may transmit the RF band signal through an antenna. The communication unit 230 downconverts an RF band signal, received through the antenna, into a baseband signal. In one example, the communication unit 310 may include a transmission filter, a reception filter, an amplifier, a mixer, an oscillator, a DAC, an ADC, or the like.

[59] The communication unit 310 may include a plurality of transmission/reception paths. In addition, the communication unit 310 may include at least one antenna array including a plurality of antenna elements. From the aspect of hardware, the communication unit 310 may include a digital circuit and an analog circuit (e.g., an RFIC). Here, the digital circuit and the analog circuit may be configured as a single package. Further, the communication unit 310 may include a plurality of RF chains. The communication unit 310 may perform beamforming.

[60] The communication unit 310 may include different communication modules to process signals in different frequency bands. Furthermore, the communication unit 310 may include a plurality of communication modules to support a plurality of different radio access technologies. For example, the different radio access technologies may include BLE, Wi-Fi, WiGig, a cellular network (e.g. LTE), and the like. The different frequency bands may include an SHF band (e.g., 2.5 GHz or 5 GHz) and a mm-wave band (e.g., 60 GHz).

[61] As described above, the communication unit 310 transmits and receives a signal. Accordingly, part or all of the communication unit 310 may be referred to as a transmitter, a receiver, or a transceiver. In the following description, transmission and reception performed through a wireless channel are construed as including processing performed as described above by the communication unit 310.

[62] The user interface unit 320 outputs information and performs functions for detecting a user's input. The user interface unit 320 may transmit a command or data input from the user to the controller 340. To this end, the user interface unit 320 may include at least one hardware module for output and input. For example, the hardware module may include at least one of a button, a lever, a sensor, a keyboard, a keypad, a speaker, a microphone, a touch screen, a liquid crystal display (LCD), a light-emitting diode (LED) display, a light-emitting polymer display (LPD), an organic light-emitting diode (OLED) display, an active-matrix organic light-emitting diode (AMOLED) display, and a flexible LED (FLED) display. The user interface unit 320 may output a

command or data received from the controller 340 through an input and output device (e.g., a speaker or a display). The user interface unit 320 displays a screen and may thus be referred to as a display unit. Further, the user interface unit 320 detects a user's input and may thus be referred to as an input unit. In some cases, the user interface unit 320 may include only a device for input, excluding a device for output.

[63] The storage unit 330 stores data, such as a default program, an application, and setting information, for the operation of the controlling terminal. The storage unit 330 may be configured as volatile memory, nonvolatile memory, or a combination of volatile memory and nonvolatile memory. The storage unit 330 provides the stored data in response to a request from the controller 340.

[64] The controller 340 controls the overall operation of the controlling terminal. For example, the controller 340 transmits and receives a signal through the communication unit 310. Further, the controller 340 may generate a control command message for controlling an aerial terminal according to a user's input and may transmit the control command message to the aerial terminal through the communication unit 310. In addition, the controller 340 records and reads data in the storage unit 330. The controller 340 may perform functions of a protocol stack required by communication standards. To this end, the controller 340 may include at least one process or micro-processor, or may be part of a processor. Part of the communication unit 310 and the controller 340 may be referred to as a CP. According to various embodiments, the controller 340 may control the controlling terminal to perform operations according to various embodiments described below.

[65] FIG. 4 illustrates the configuration of a core network device in a wireless communication system according to various embodiments. The configuration illustrated in FIG. 4 may be understood as the configuration of a device having at least one function of the UTM 170, the regulator 190, the SMF, the AMF, the PCF, and the UDM described with reference to FIG. 1. The terms 'unit', '-or/er', and the like used herein indicate a unit for processing at least one function or operation, which may be implemented as hardware, software, or a combination thereof.

[66] Referring to FIG. 4, the core network device includes a communication unit 410, a storage unit 420, and a controller 430.

[67] The communication unit 410 provides an interface for performing communication with other devices in a network. That is, the communication unit 410 converts a bit stream which is transmitted from the core network device to a different device into a physical signal and converts a physical signal which is received from a different device into a bit stream. That is, the communication unit 410 may transmit and receive a signal. Accordingly, the communication unit 410 may be referred to as a modem, a transmitter, a receiver, or a transceiver. Here, the communication unit 410 enables the

core network device to communicate with other devices or systems via backhaul (e.g., wired backhaul or wireless backhaul) connection or via the network.

[68] The storage unit 420 stores data, such as a default program, an application, and setting information, for the operation of the core network device. The storage unit 420 may be configured as volatile memory, nonvolatile memory, or a combination of volatile memory and nonvolatile memory. The storage unit 420 provides the stored data in response to a request from the controller 430.

[69] The controller 430 controls the overall operation of the core network device. For example, the controller 430 transmits and receives a signal through the communication unit 410. Further, the controller 430 records and reads data in the storage unit 420. To this end, the controller 430 may include at least one process. According to various embodiments, the controller 430 may control the core network device to perform operations according to various embodiments described below.

[70] FIG. 5 is a flowchart 500 illustrating the operation of an access management function (AMF) in a wireless communication system according to various embodiments. FIG. 5 illustrates an operating method of a device for the AMF.

[71] Referring to FIG. 5, in operation 501, the AMF receives a registration request message associated with a UAS from a UAS terminal. In operation 503, the AMF performs a process of authenticating the UAS terminal. In operation 505, the AMF requests registration of the UAS terminal from a UDM. In operation 507, the AMF receives a response to a registration request of the UAS terminal from the UDM. In operation 509, the AMF determines whether to perform additional authentication. In operation 511, the AMF requests UAS authentication of the UAS terminal from a UTM. In operation 513, the AMF receives a result of UAS authentication of the UAS terminal from the UTM. In operation 515, the AMF transmits a registration acceptance message to the UAS terminal.

[72] FIG. 6 is a flowchart 600 illustrating the operation of a UAS traffic management (UTM) in a wireless communication system according to various embodiments. FIG. 6 illustrates an operating method of a device for the UTM.

[73] Referring to FIG. 6, in operation 601, the UTM receives a request for UAS authentication associated with a UAS from an access management function (AMF). In operation 603, the UTM identifies a pair of paired UAS terminals. In operation 605, the UTM identifies whether pairing tokens match. In operation 607, the UTM performs a UAS authentication process. In operation 609, the UTM transmits a result of UAS authentication of the UAS terminals to the AMF.

[74] FIG. 7 is a flowchart 700 illustrating the operation of a UAS terminal in a wireless communication system according to various embodiments. FIG. 7 illustrates an operating method of the aerial terminal 115 or the controlling terminal 113.

[75] Referring to FIG. 7, in operation 701, the UAS terminal performs pairing with a different UAS terminal. To this end, the UAS terminal may generate a pairing token and may exchange the pairing token with the different UAS terminal. Accordingly, the UAS terminal may perform mutual authentication and recognition with the different UAS terminal. Here, the pairing token is a unique value shared between the UAS terminals which are mutually paired for a UAS and may be used as information for proving a pairing relationship in subsequent operations. In operation 703, the UAS terminal transmits a registration request message to an AMF. In operation 705, the UAS terminal receives a registration acceptance message from the AMF.

[76] FIG. 8 is a signal exchange diagram showing that a UAS terminal performs authentication for a UAS in a wireless communication system according to various embodiments. Here, the UAS terminal may be understood as either the foregoing aerial terminal or the foregoing controlling terminal. In the following description, the aerial terminal is referred to as a UAV, and the controlling terminal is referred to as a UAC.

[77] FIG. 8 illustrates a procedure in which a UTM 880 receives information required for authentication of a UAS terminal from the terminal and a mobile communication system and performs authentication for a UAS in initial access of the terminal to the mobile communication network, in which specific messages may be changed according to a configuration.

[78] Referring to FIG. 8, in operation 801, the UAS terminal, that is, a UAV 810 and a UAC 820, performs authentication and recognition operations to each other according to a predetermined pairing method in order to mutually transmit and receive flight and control information. As a pairing method to be used, various methods may be applied depending on configurations and products, among which a public key-based authentication method using a short-range transmission technology, such as Wi-Fi or Bluetooth, or a certificate-based authentication method using a certificate issued by a certification authority may generally be applied. For example, in operation 801a, operation 801b, and operation 801c, the UAV 810 and the UAC 820 generate and exchange a pairing token for distinguishing pairing between the UAV 810 and the UAC 820 in a subsequent UAS authentication process during a pairing process.

[79] In operation 802 and operation 803, the UAV 810 and the UAC 820 transmit a registration request message to a mobile communication network in order to perform an initial registration process with the network. Here, the terminal includes UAS information, which is additional information for a UAS, in the registration request message, and the UAS information may include the identifier of a corresponding terminal used for the UAS, the identifier of a paired terminal (including a plurality of identifiers when controlling a plurality of UAVs 810 at the same time), the UAS terminal type of the corresponding terminal (e.g., information for identifying the UAV

810 or the UAC 820), pairing token information, and the like. According to an alternative provided method, when the terminal does not need to use the UAS through an initial access process, it is possible to omit the UAS information and to request authentication for the UAS through a protocol data unit (PDU) session generation request at a required time after completing initial access.

[80] In operation 804, upon receiving the registration request message from each UAS terminal, each AMF 840 performs an authentication process necessary for use of a mobile communication system with each UAS terminal. When an authentication operation is successfully completed, the AMF 840 stores the terminal in a user data management (UDM) 860 and receives subscription information about the terminal from the UDM 860 in operation 805. The AMF 840 identifies that the terminal is a UAS terminal based on a user equipment (UE) type transmitted from the terminal or UE type information included in the subscription information about the terminal received from the UDM 860. In operation 806, the AMF 840 determines that it is needed to perform an additional authentication process for UAS authorization for the UAS terminal with the UTM 880. In operation 807, the AMF 840 transmits an UAS authorization request control message to a UTM 880, thereby requesting authentication of the UAS terminal for the UAS. The UAS authorization request message may include a generic public subscription identifier (GPSI), which is the external network identifier of the terminal, and information included in the UAS information received by the AMF 840 from the terminal, that is, the UAS ID, the paired UAS ID, the UAS type, and the pairing token information, and may further include an international mobile station identity (IMSI), which is the internal network identifier of the terminal, service area information, subscription information, and the like.

[81] In operation 808, the UTM 880 identifies a pair of paired UAS terminals from the UAS ID and the paired UAS ID included in the UAS authorization request message received from each AMF 840 and identifies whether the forwarded pairing tokens match. In operation 809, operation 811-1, and operation 811-2, when the pieces of pairing information match, the UTM 880 performs an authentication process for authorizing the UAS with each terminal. After completing the authentication process for the UAS, the UTM 880 transmits a UAS authorization acceptance message including the authentication result for the UAS to the AMF 840 in operation 812. The UAS authorization acceptance message includes the GPSI and the UAS information received from the AMF 840 as information for identifying the terminal and may additionally include the IP address of the terminal, allowed UAS area information, a reporting condition for a UAS location (status) change, and the like.

[82] In operation 813, the UTM 880 may transmit a UAS policy request message for requesting UAS policy updating according to UAS initiation to a policy control function

(PCF) 850 of the mobile communication network. The UAS policy request message may include the GPSI, which is the external identifier of the terminal, the UAS information, a terminal IP address, a UAS area, and quality of service (QoS) information required by the UAS.

[83] In operation 814, the PCF 850 transmits a control message delivering updated policy information to a session management function (SMF) 830 when policy updating is needed based on the information included in the UAS policy request message received from the UTM 880.

[84] In operation 815 and operation 816, the AMF 840 configures UAS-related information from the UAS-related information received from the UTM 880 and transmits the UAS-related information to the terminal through a registration acceptance message. Here, the UAS-related information may include an internal identifier or an external identifier of a mobile communication network of a paired counterpart terminal, a UAS identifier of the paired counterpart terminal, the IP address of the counterpart terminal for the UAS, and QoS information used for the UAS.

[85] FIG. 9 is a signal exchange diagram showing that a UAS terminal performs initial access in a wireless communication system according to various embodiments. FIG. 9 illustrates an example of applying the provided method, in which at least one of UAS terminals does not transmit UAS information through a registration request message when pairing between UAS terminals is not completed or the UAS terminal does not require a flight request yet during a registration process for initial access.

[86] Referring to FIG. 9, in operation 901, the UAS terminal, that is, a UAV 910 and a UAC 920, performs authentication and recognition operations to each other according to a predetermined pairing method in order to mutually transmit and receive flight and control information. As a pairing method to be used, various methods may be applied depending on configurations and products, among which a public key-based authentication method using a short-range transmission technology, such as Wi-Fi or Bluetooth, or a certificate-based authentication method using a certificate issued by a certification authority may generally be applied. For example, in operation 901a, operation 901b, and operation 901c, the UAV 910 and the UAC 920 generate and exchange a pairing token for distinguishing pairing between the UAV 910 and the UAC 920 in a subsequent UAS authentication process during a pairing process.

[87] In operation 902 and operation 903, each of the UAV 910 and UAC 920 transmits a registration request message including a control parameter designating a UE type to a UAV or a UAC to an AMF 940 in order to indicate that each of the UAV 910 and UAC 920 is a UAS terminal. Here, the UAV 910 and the UAC 920 may perform a registration process through different AMFs 940 according to a configuration and a network configuration environment. According to a configuration, when UE type in-

formation is previously stored as subscriber information in a wireless network, the terminal may omit a UE type parameter from the registration request message. In operation 904, the AMF 940 analyzes the received registration request message and performs a necessary registration process. That is, the AMF 940 controls the UAV 910 and the UAC 920 to perform an authentication process through a UDM 960. When authentication is successfully completed, the AMF 940 registers the UAV 910 and the UAC 920 in the UDM 960 and receives subscription information about a terminal from the UDM 960 in operation 905. In operation 906, the AMF 940 transmits a policy request message to the UDM 960 and receives a policy response message from the UDM 960. The policy request message may include a UE ID, an MM policy, and the like. When the registration request message does not include a UE type parameter, the AMF 940 may identify that the terminal is a UAS terminal through a UE type parameter included in the subscription information received from the UDM 960. When the registration request message does not include a UE type and subscription information about a corresponding terminal received from the UDM 960 does not include a UE type parameter, the AMF 940 cannot determine that the terminal is a UAS terminal. In this case, the terminal may be regarded as a general terminal rather than a UAS terminal. When the registration process is successfully completed, the AMF 940 transmits a registration acceptance message to the terminal in operation 907.

[88] FIG. 10 is a signal exchange diagram showing that a UAS terminal having completed access performs authentication for a UAS in order to use the UAS in a wireless communication system according to various embodiments.

[89] Referring to FIG. 10, in operation 1001, the UAS terminal, that is, a UAV 1010 and a UAC 1020, performs authentication and recognition operations to each other according to a predetermined pairing method in order to mutually transmit and receive flight and control information. As a pairing method to be used, various methods may be applied depending on configurations and products, among which a public key-based authentication method using a short-range transmission technology, such as Wi-Fi or Bluetooth, or a certificate-based authentication method using a certificate issued by a certification authority may generally be applied. For example, in operation 1001a, operation 1001b, and operation 1001c, the UAV 1010 and the UAC 1020 generate and exchange a pairing token for distinguishing pairing between the UAV 1010 and the UAC 1020 in a subsequent UAS authentication process during a pairing process.

[90] In operation 1002, the UAS terminal transmits a PDU session establishment request control message to a mobile communication network in order to generate a PDU session for a UAS. When there is a plurality of UTMs 1080 supporting the UAS, the UAS terminal may transmit a PDU session establishment request message including the ID of a UTM 1080 suitable for the UAS which the UAS terminal wants to use. In

operation 1003, after receiving the PDU session establishment request message, an SMF 1030 transmits a PCF association request control message for requesting determination of a policy for a corresponding session to a PCF, and this message may include a terminal identifier received from the UAS terminal, a DNN, request slice information (S-NSSAI), the identifier of the UTM 1080, and the like. In operation 1004, the SMF 1030 receives a PCF association response message from the PCF 1050. In operation 1005, the SMF 1030 determines that secondary authorization is required for a session request from the UAS terminal based on SM policy information included in the PCF association response message.

[91] In operation 1006, the SMF 1030 transmits a DN authorization request message for requesting secondary authorization to the UTM 1080. The DN authorization request message includes a GPSI, which is the external network identifier of the terminal, and UAS information. In operation 1007-1 and operation 1007-2, the UAV 1010 performs a UAS authentication process. When pairing information is not forwarded to the UTM 1080 in a registration process of the UAS terminal, the UAS terminal may transmit the pairing information to the UTM 1080 by including the pairing information in the PDU session establishment request message or by including the pairing information as a parameter of a control message in the UAS authentication process. In operation 1008, during the authentication process, the UTM 1080 identifies information about a paired terminal from the terminal and compares pieces of pairing token information received from the two UAS terminals, thereby identifying the status of pairing between the UAV 1010 and the UAC 1020. In operation 1009, the UTM 1080 determines whether to authorize the pairing and the UAS based on UAS subscription information about the corresponding terminal stored in the UTM 1080. In operation 1011, the UTM 1080 transmits a policy update request message to the PCF 1050 and receives a policy update response message from the PCF 1050. The policy update request message may include a UE ID, UAS information, and information about a paired counterpart terminal. In operation 1011 and operation 1012, the UTM 1080 transmits (1011 and 1012) the result of authorization for the UAS request from the UAS terminal and UAS-related information (e.g., a GPSI, the identifier of a paired counterpart terminal, the IP address of the counterpart terminal, a UAS area, and the like) to the PCF 1050 and the SMF 1030 through separate control messages. In operation 1003, the SMF 1030 requests policy information about a PDU session from the PCF 1050 and receives SM policy information to be applied to the UAS from the PCF 1050. The SMF 1030 can control the PDU session to be limited to be used for the UAS based on the received UAS-related information, and can limit the PDU session to be used only for communication between the UAV 1010 and the UAC and communication between the UAV 1010 (or the UAC) and the UTM 1080 if necessary.

[92] In operation 1014, the SMF 1030 transmits a PDU session establishment response message to the UAS terminal first receiving the PDU session establishment request among the UAV 1010 and the UAC. Here, the newly generated PDU session may be configured to be in a deactivated state until the paired counterpart UAS terminal completes the PDU session according to a configuration and may be controlled by a session state parameter included in the PDU session establishment response message.

[93] In operation 1015, the UAC 1020 performs a PDU session establishment process for using the UAS, including the authentication process with the UTM 1080. In operation 1016, the SMF 1030 repeats the same PDU session establishment process with a second UAS terminal, and when the process is successfully completed, the SMF 1030 transmits a PDU session modification request message including session state information with session state = activate to a first UAS terminal, thereby controlling the first UAS terminal to activate the state of the PDU session for the UAS and to use the PDU session for the UAS.

[94] When the pairing status between the UAS terminals is updated during the UAS, it is possible for the UAS terminal to perform re-authentication with the UTM 1080 using the UAS authentication process illustrated in FIG. 8 or FIG. 9 and FIG. 10 according to UAS provider policies.

[95] The effects obtainable from the disclosure are not limited to the effects mentioned above, and other effects not mentioned will be clearly understood by those skilled in the art from the following description.

[96] Methods according to embodiments illustrated in the claims or specification may be implemented by hardware, software, or a combination of hardware and software.

[97] When the methods are implemented by software, a computer-readable storage medium storing one or more programs (software modules) may be provided. One or more programs stored in the computer-readable storage medium are configured for execution by one or more processors in an electronic device. The one or more programs include instructions that enable the electronic device to execute the methods according to the embodiments illustrated in the claims or specification.

[98] These programs (software modules or software) may be stored in a random-access memory, a nonvolatile memory including a flash memory, a read-only memory (ROM), an electrically erasable programmable ROM (EEPROM), a magnetic disc storage device, a compact disc ROM (CD-ROM), digital versatile discs (DVDs), an optical storage device in a different form, a magnetic cassette, or a memory configured in a combination of some or all thereof. In addition, each constituent memory may be included in plural.

[99] Further, the programs may be stored in an attachable storage device which is accessible through a communication network, such as the Internet, an intranet, a local

area network (LAN), a wide area network (WAN), or a storage area network (SAN), or a communication network configured in a combination thereof. This storage device may be connected to a device for performing an embodiment through an external port. In addition, a separate storage device on a communication network may be connected to a device for performing an embodiment.

[100] In the specific embodiments of the disclosure described above, components included in the disclosure are expressed in a singular form or a plural form according to the illustrated specific embodiments. However, singular or plural expressions are appropriately selected for illustrated situations presented for convenience of explanation, and the disclosure is not limited to singular or plural components. A plural expression of a component may include one component or a singular expression of a component may include a plurality of components.

[101] Although specific embodiments have been illustrated in the detailed description of the disclosure, different modifications may be possible without departing from the scope of the disclosure. Therefore, the scope of the disclosure will be defined not by the described embodiments but by the appended claims to be mentioned and equivalents thereto.

[102] Although the present disclosure has been described with various embodiments, various changes and modifications may be suggested to one skilled in the art. It is intended that the present disclosure encompass such changes and modifications as fall within the scope of the appended claims.

Claims

[Claim 1] A method performed by an apparatus for an access management function (AMF) in a wireless communication system, the method comprising:
receiving, from a terminal, a registration request message associated with an unmanned aerial service (UAS) of the terminal;
performing an authentication process of the terminal;
transmitting, to a user data management (UDM), a request for a registration of the terminal;
receiving, from the UDM, a response to the request for the registration of the terminal ;
determining whether to perform additional authentication based on the response to the request for the registration of the terminal;
transmitting, to a UAS traffic management (UTM), a request for a UAS authentication of the terminal;
receiving, from the UTM, a result of the UAS authentication of the terminal; and
transmitting, to the terminal, a registration acceptance message based on the results of the UAS authentication of the terminal.

[Claim 2] The method of claim 1, wherein the registration request message comprises UAS information, and the UAS information comprises an identifier of the terminal, a terminal type of the terminal, and pairing information associated with the terminal.

[Claim 3] The method of claim 2, wherein transmitting the request for the UAS authentication of the terminal comprises transmitting, to the UTM, a UAS authority request message, and the UAS authority request message comprises the UAS information.

[Claim 4] The method of claim 1, wherein the registration acceptance message is transmitted along with UAS-related information, and the UAS-related information comprises identifier information associated with a paired counterpart terminal.

[Claim 5] A method performed by an apparatus for an unmanned aerial service (UAS) traffic management (UTM) in a wireless communication system, the method comprising:
receiving, from an access management function (AMF), a request for authentication associated with the UAS;
identifying a pair of paired terminals based on the request for the au-

thentication associated with the UAS;
determining whether pairing tokens match based on the pair of paired terminals;
performing a UAS authentication process based on a determination that the pairing tokens match; and
transmitting, to the AMF, a result of the UAS authentication process of a terminal.

[Claim 6] The method of claim 5, wherein receiving the request for the authentication associated with the UAS comprises receiving, from the AMF, a UAS authority request message, the UAS authority request message comprises UAS information, and the UAS information comprises an identifier of the terminal, a terminal type of the terminal, and pairing information associated with the terminal.

[Claim 7] The method of claim 5, further comprising transmitting, to a policy control function (PCF), a request for updating UAS policy.

[Claim 8] A method performed by a terminal in a wireless communication system, the method comprising:
performing mutual authentication with a different terminal based on a predetermined pairing scheme;
transmitting, to an access management function (AMF), a request for a registration associated with an unmanned aerial service (UAS); and
receiving, from the AMF, a result of the request for the registration associated with the UAS.

[Claim 9] The method of claim 8, wherein performing the mutual authentication with the different terminal based on the predetermined pairing scheme comprises generating a pairing token and exchanging the generated pairing token with the different terminal.

[Claim 10] The method of claim 9, wherein transmitting the request for the registration associated with the UAS comprises transmitting, to the AMF, a registration request message, and the registration request message comprises an identifier of the terminal, an identifier of the different terminal paired with the terminal, UAS terminal types of the terminal and the different terminal paired with the terminal, and information associated with the pairing token.

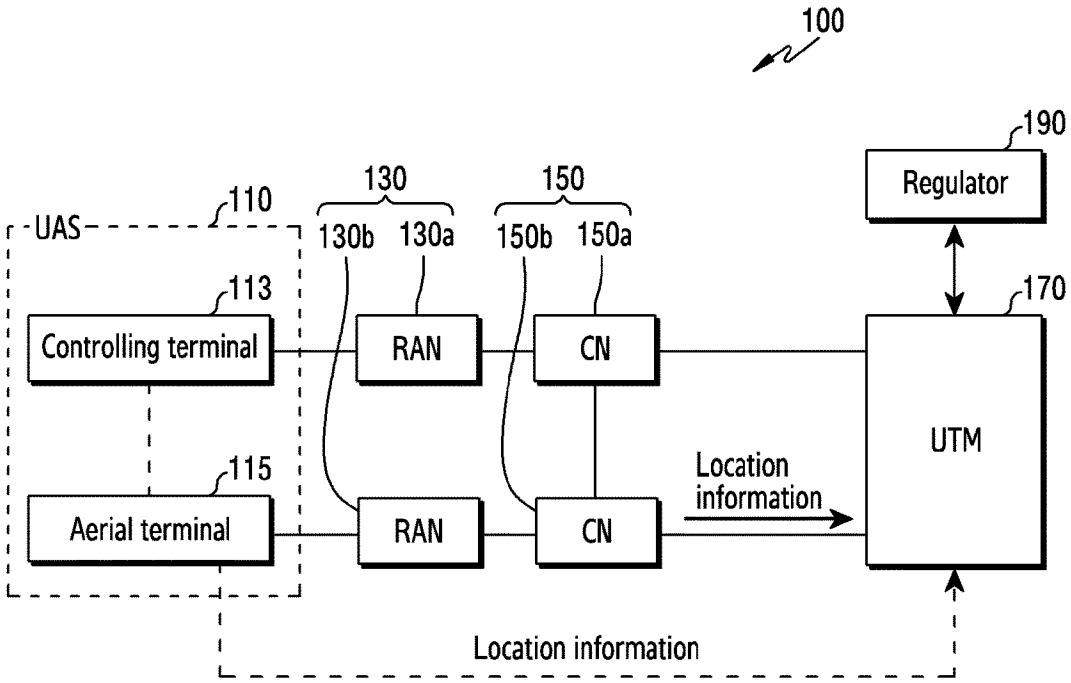
[Claim 11] An apparatus for an access management function (AMF) in a wireless communication system, the apparatus configured to implement the method of one of claims 1 to 4.

[Claim 12] An apparatus for an unmanned aerial service (UAS) traffic

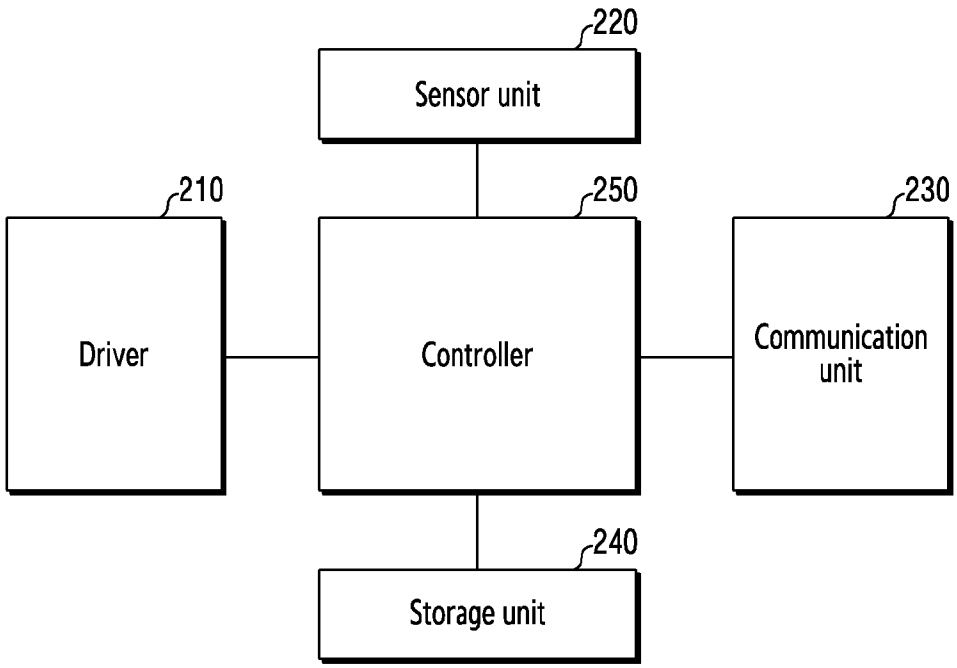
management (UTM) in a wireless communication system, the apparatus configured to implement the method of one of claims 5 to 7.

[Claim 13] An apparatus of a terminal, the apparatus configured to implement the method of one of claims 8 to 10.

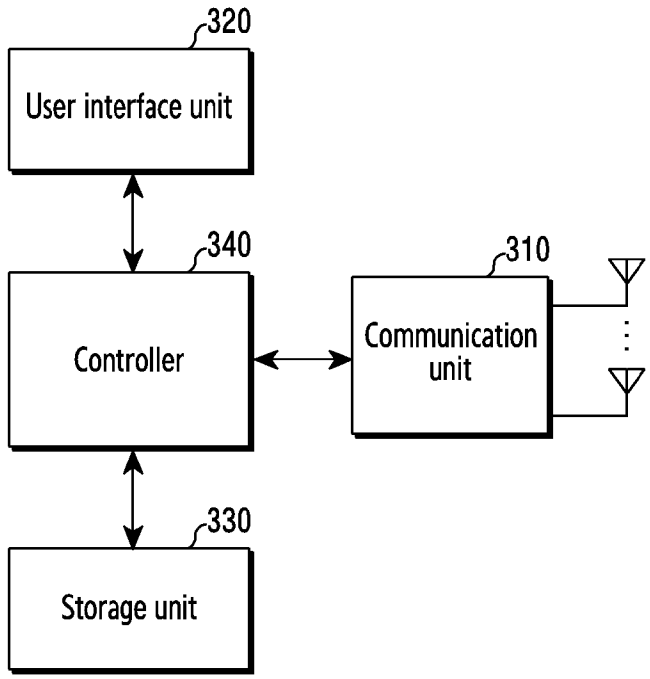
[Fig. 1]


100
190
Regulator
130
150
110
UAS
130b
130a
150b
150a
113
170
Controlling terminal
RAN
CN
UTM
115
Location information
Aerial terminal
RAN
CN
Location information

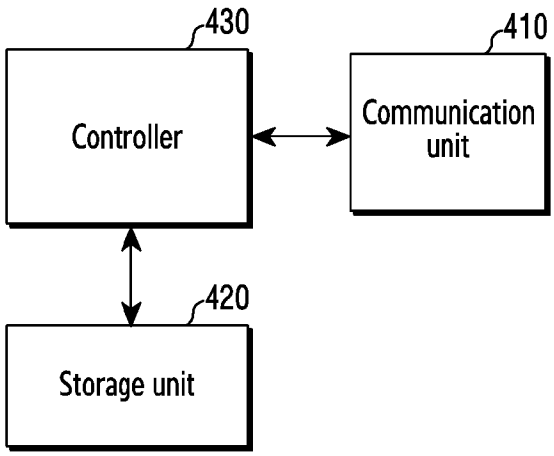
[Fig. 2]


220
Sensor unit
210
250
230
Driver
Controller
Communication unit
240
Storage unit

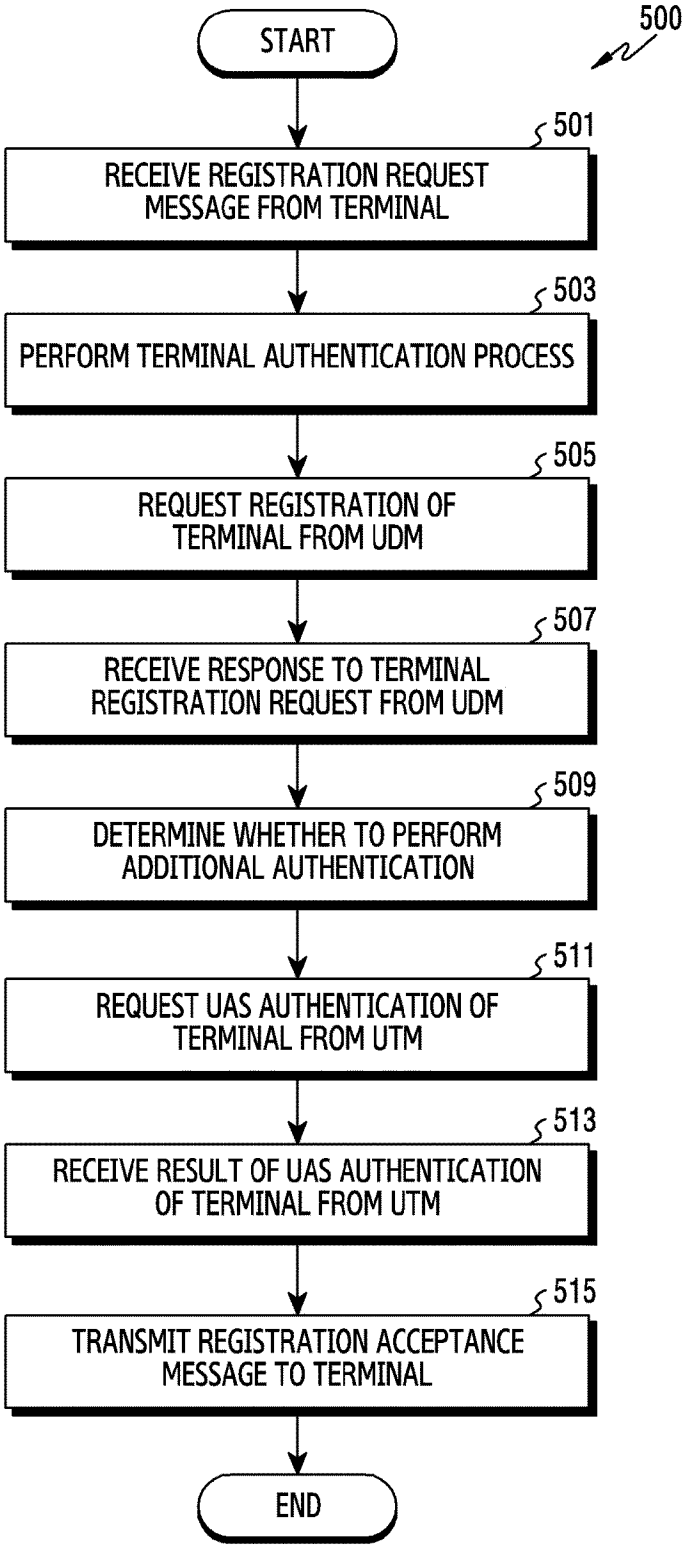
[Fig. 3]


320
User interface unit
340
Controller
310
Communication unit
330
Storage unit

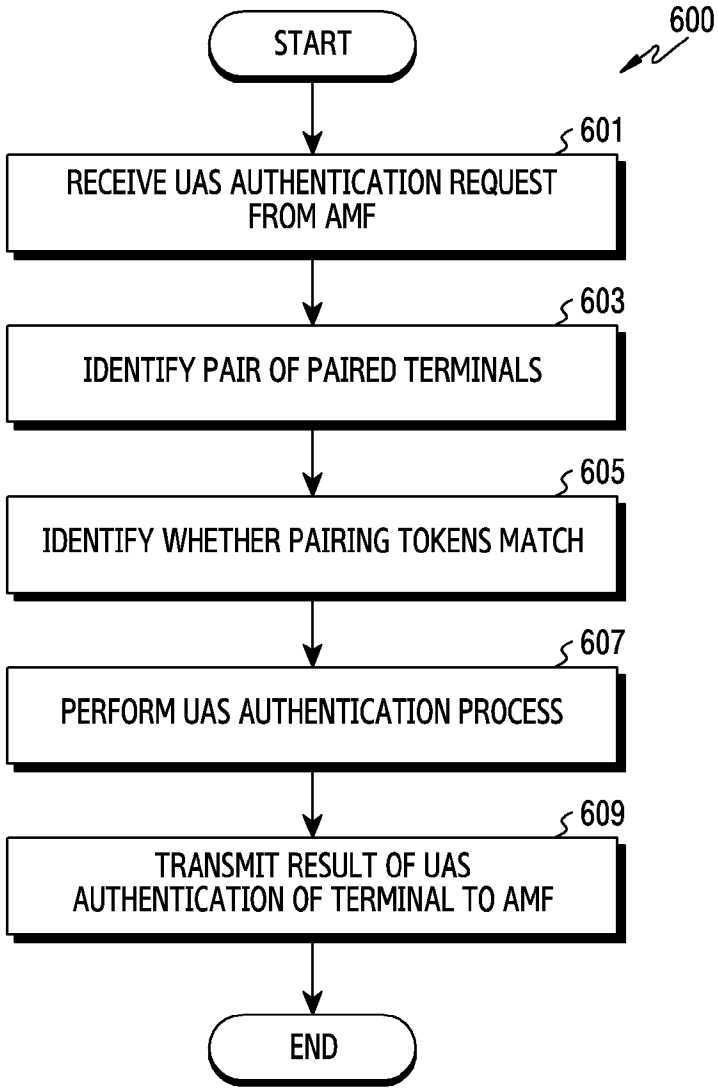
[Fig. 4]


430
Controller
410
Communication unit
420
Storage unit

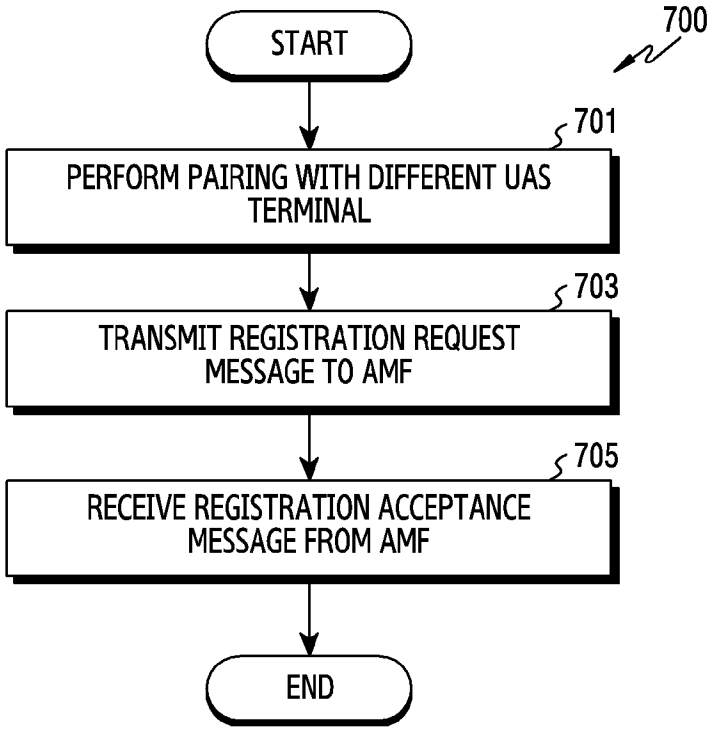
[Fig. 5]


500
START
501
RECEIVE REGISTRATION REQUEST MESSAGE FROM TERMINAL
503
PERFORM TERMINAL AUTHENTICATION PROCESS
505
REQUEST REGISTRATION OF TERMINAL FROM UDM
507
RECEIVE RESPONSE TO TERMINAL REGISTRATION REQUEST FROM UDM
509
DETERMINE WHETHER TO PERFORM ADDITIONAL AUTHENTICATION
511
REQUEST UAS AUTHENTICATION OF TERMINAL FROM UTM
513
RECEIVE RESULT OF UAS AUTHENTICATION OF TERMINAL FROM UTM
515
TRANSMIT REGISTRATION ACCEPTANCE MESSAGE TO TERMINAL
END

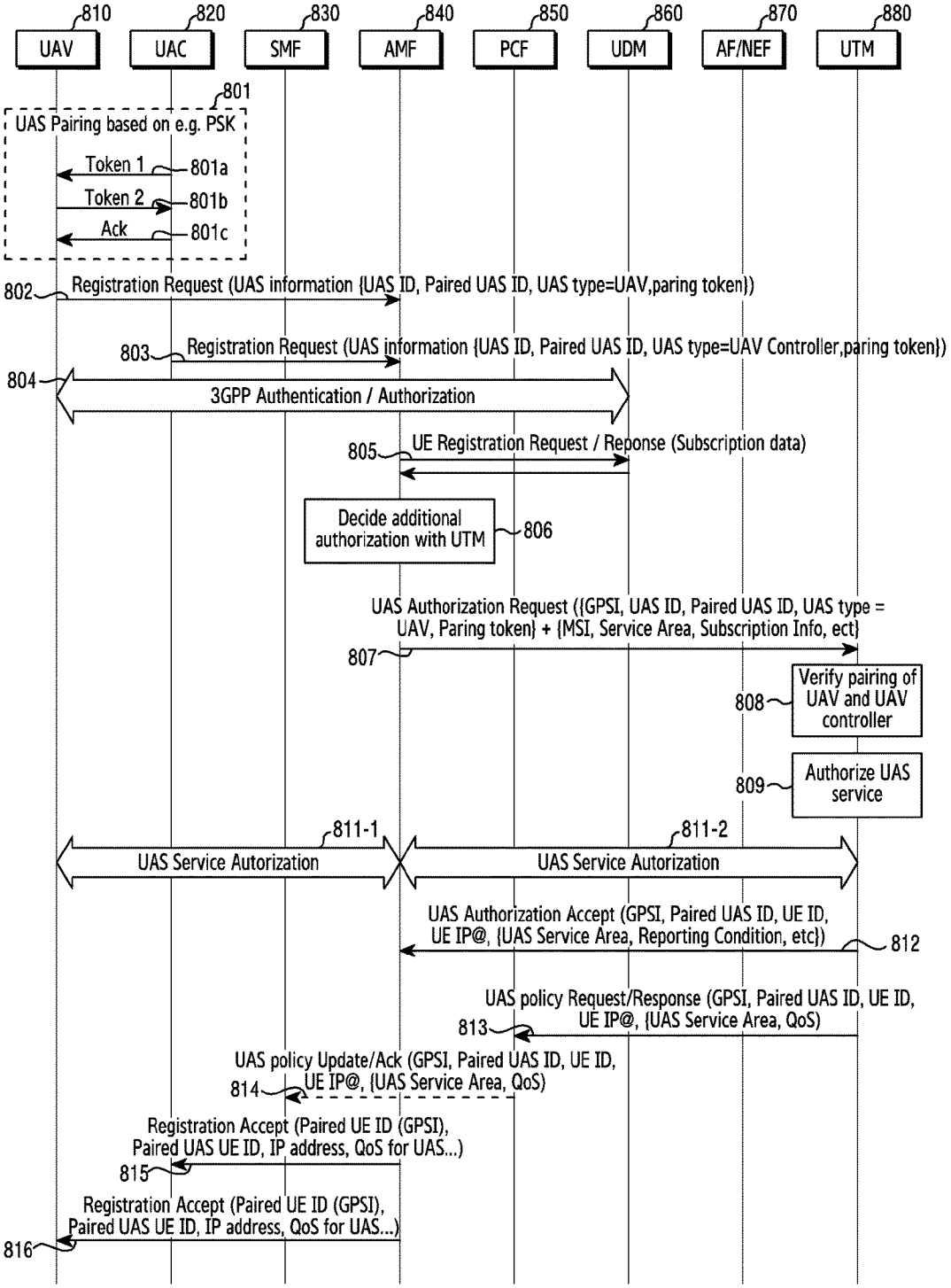
[Fig. 6]


600
START
601
RECEIVE UAS AUTHENTICATION REQUEST FROM AMF
603
IDENTIFY PAIR OF PAIRED TERMINALS
605
IDENTIFY WHETHER PAIRING TOKENS MATCH
607
PERFORM UAS AUTHENTICATION PROCESS
609
TRANSMIT RESULT OF UAS AUTHENTICATION OF TERMINAL TO AMF
END

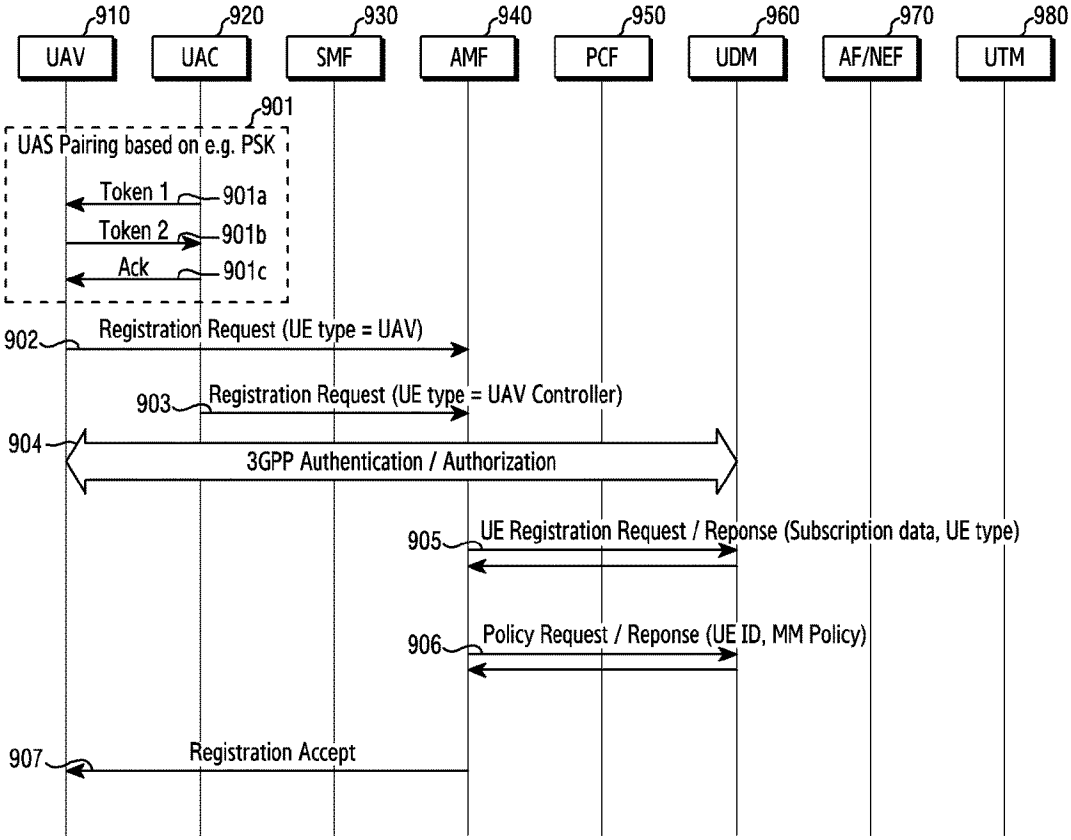
[Fig. 7]


700
START
701
PERFORM PAIRING WITH DIFFERENT UAS TERMINAL
703
TRANSMIT REGISTRATION REQUEST MESSAGE TO AMF
705
RECEIVE REGISTRATION ACCEPTANCE MESSAGE FROM AMF
END

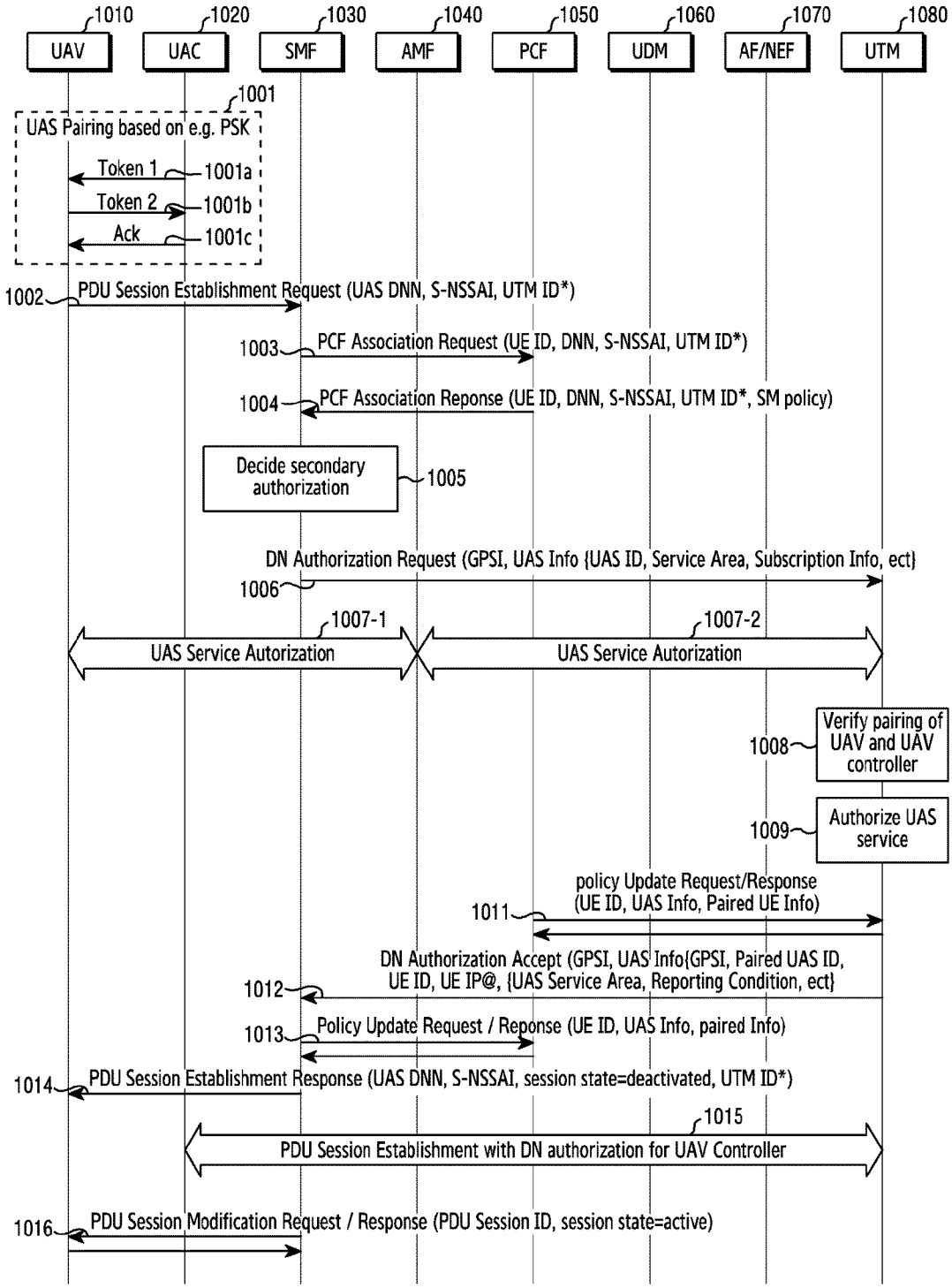
[Fig. 8]


810
UAV
820
UAC
830
SMF
840
AMF
850
PCF
860
UDM
870
AF/NEF
880
UTM
801
UAS Pairing based on e.g. PSK
Token 1
801a
Token 2
801b
Ack
801c
802
Registration Request (UAS information {UAS ID, Paired UAS ID, UAS type=UAV,paring token})
803
Registration Request (UAS information {UAS ID, Paired UAS ID, UAS type=UAV Controller,paring token})
804
3GPP Authentication / Authorization
805
UE Registration Request / Reponse (Subscription data)
Decide additional authorization with UTM
806
UAS Authorization Request ({GPSI, UAS ID, Paired UAS ID, UAS type = UAV, Paring token} + {MSI, Service Area, Subscription Info, ect}
807
Verify pairing of UAV and UAV controller
808
Authorize UAS service
809
811-1
UAS Service Autorization
811-2
UAS Service Autorization
UAS Authorization Accept (GPSI, Paired UAS ID, UE ID, UE IP@, {UAS Service Area, Reporting Condition, etc})
812
UAS policy Request/Response (GPSI, Paired UAS ID, UE ID, UE IP@, {UAS Service Area, QoS)
813
UAS policy Update/Ack (GPSI, Paired UAS ID, UE ID, UE IP@, {UAS Service Area, QoS)
814
Registration Accept (Paired UE ID (GPSI), Paired UAS UE ID, IP address, QoS for UAS...)
815
Registration Accept (Paired UE ID (GPSI), Paired UAS UE ID, IP address, QoS for UAS...)
816

[Fig. 9]


910
UAV
920
UAC
930
SMF
940
AMF
950
PCF
960
UDM
970
AF/NEF
980
UTM
901
UAS Pairing based on e.g. PSK
Token 1
901a
Token 2
901b
Ack
901c
902
Registration Request (UE type = UAV)
903
Registration Request (UE type = UAV Controller)
904
3GPP Authentication / Authorization
905
UE Registration Request / Reponse (Subscription data, UE type)
906
Policy Request / Reponse (UE ID, MM Policy)
907
Registration Accept

[Fig. 10]


1010
UAV
1020
UAC
1030
SMF
1040
AMF
1050
PCF
1060
UDM
1070
AF/NEF
1080
UTM
1001
UAS Pairing based on e.g. PSK
Token 1
1001a
Token 2
1001b
Ack
1001c
1002
PDU Session Establishment Request (UAS DNN, S-NSSAI, UTM ID*)
1003
PCF Association Request (UE ID, DNN, S-NSSAI, UTM ID*)
1004
PCF Association Reponse (UE ID, DNN, S-NSSAI, UTM ID*, SM policy)
Decide secondary authorization
1005
DN Authorization Request (GPSI, UAS Info {UAS ID, Service Area, Subscription Info, ect}
1006
1007-1
UAS Service Autorization
1007-2
UAS Service Autorization
Verify pairing of UAV and UAV controller
1008
Authorize UAS service
1009
policy Update Request/Response (UE ID, UAS Info, Paired UE Info)
1011
DN Authorization Accept (GPSI, UAS Info{GPSI, Paired UAS ID, UE ID, UE IP@, {UAS Service Area, Reporting Condition, ect}
1012
1013
Policy Update Request / Reponse (UE ID, UAS Info, paired Info)
1014
PDU Session Establishment Response (UAS DNN, S-NSSAI, session state=deactivated, UTM ID*)
1015
PDU Session Establishment with DN authorization for UAV Controller
1016
PDU Session Modification Request / Response (PDU Session ID, session state=active)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2020/012175

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/06(2009.01)i; **H04W 8/24**(2009.01)i; **H04W 60/00**(2009.01)i; **H04W 4/40**(2018.01)i; **H04W 84/06**(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W 12/06(2009.01); G05D 1/10(2006.01); G08G 5/00(2006.01); H04L 29/06(2006.01); H04W 12/08(2009.01); H04W 4/12(2009.01); H04W 60/00(2009.01); H04W 76/04(2009.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: AMF, UTM, UAS, authentication, registration

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2016-0285864 A1 (AMAZON TECHNOLOGIES, INC.) 29 September 2016 (2016-09-29) paragraphs [0092]-[0094], [0109]; and claims 1-20	8-10,13
A		1-7,11,12
Y	WO 2017-142362 A1 (LG ELECTRONICS INC.) 24 August 2017 (2017-08-24) claims 1-12; and figure 10	8-10,13
Y	US 9412278 B1 (SZ DJI TECHNOLOGY CO., LTD) 09 August 2016 (2016-08-09) column 8, lines 51-67; column 24, lines 53-67; and claims 1-24	9,10
A	WO 2018-008983 A1 (SAMSUNG ELECTRONICS CO., LTD.) 11 January 2018 (2018-01-11) paragraphs [0209]-[0212]; and claims 1-7	1-13
A	US 2016-0275801 A1 (USA AS REPRESENTED BY THE ADMINISTRATOR OF THE NATIONAL AERONAUTICS & SPACE ADMINISTRATION (NASA)) 22 September 2016 (2016-09-22) paragraphs [0166]-[0173]; and claims 1-20	1-13

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 December 2020	**15 December 2020**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**YANG JEONG ROK**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5709**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2020/012175

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2016-0285864 A1	29 September 2016	CA 2980747 A1	06 October 2016
		CA 2980747 C	09 June 2020
		CN 107438989 A	05 December 2017
		CN 107438989 B	11 August 2020
		EP 3275154 A1	31 January 2018
		JP 2018-511248 A	19 April 2018
		JP 6628372 B2	08 January 2020
		US 2016-0280370 A1	29 September 2016
		US 2016-0280371 A1	29 September 2016
		US 2016-0285863 A1	29 September 2016
		US 2018-0198779 A1	12 July 2018
		US 9663226 B2	30 May 2017
		US 9714088 B2	25 July 2017
		US 9912655 B2	06 March 2018
		US 9930027 B2	27 March 2018
		WO 2016-160593 A1	06 October 2016
WO 2017-142362 A1	24 August 2017	CN 108702722 A	23 October 2018
		EP 3419351 A1	26 December 2018
		US 2019-0037636 A1	31 January 2019
US 9412278 B1	09 August 2016	CN 107409051 A	28 November 2017
		EP 3254404 A1	13 December 2017
		JP 2017-526280 A	07 September 2017
		JP 6423521 B2	14 November 2018
		US 2016-0288905 A1	06 October 2016
		US 2016-0292403 A1	06 October 2016
		US 2016-0292696 A1	06 October 2016
		US 2017-0169713 A1	15 June 2017
		US 2018-0082308 A1	22 March 2018
		US 2018-0211263 A1	26 July 2018
		US 9792613 B2	17 October 2017
		US 9805372 B2	31 October 2017
		US 9805607 B2	31 October 2017
		US 9870566 B2	16 January 2018
		WO 2016-154949 A1	06 October 2016
WO 2018-008983 A1	11 January 2018	CN 109417709 A	01 March 2019
		EP 3466135 A1	10 April 2019
		KR 10-2019-0016540 A	18 February 2019
		US 10716002 B2	14 July 2020
		US 2019-0261178 A1	22 August 2019
US 2016-0275801 A1	22 September 2016	US 10332405 B2	25 June 2019